GESTÃO DA SEGURANÇA DA INFORMAÇÃO: UMA SOLUÇÃO CONTRA O VAZAMENTO DE INFORMAÇÕES CORPORATIVAS, CAUSADO PELOS DISPOSITIVOS AMOVÍVEIS.[1]

Michele Peruci[2]
Paulo Sérgio Montagnana[3]
Simone da Silveira[4]

RESUMO: O propósito deste artigo é contribuir com o leitor, apresentando uma visão da importância da segurança da informação, dentro de um referencial de gestão de riscos que vem ocorrendo devido às novas tecnologias de dispositivos amovíveis, como pen drives, celulares, smartphones, palmtops, disquetes, bluetooth, gravadores de CD/DVD, modem 3G, enfim, a lista destes equipamentos a disposição no mercado são enormes, e seu uso devido à fácil portabilidade de informações só cresce. Proporcionalmente, cresce também os riscos de vazamento de dados.

Assim sendo, este artigo procura também levar ao conhecimento do leitor uma solução desenvolvida pela empresa Makrosystems – Tecnologia de Informação, com sede em Canoinhas, Santa Catarina, apresentando um novo modelo de software que tem a finalidade de proteger o vazamento de informações corporativas, ocorridas através destes dispositivos amovíveis.
Palavras Chaves: Segurança da informação – Dispositivos amovíveis – Fuga de dados

ABSTRACT: The purpose of this article is to contribute for the reader, presenting a sight of the importance of security information, within a benchmark for risk management that has occurred due to new technologies for removable devices such as pen drives, cell phones, smartphones, palmtops, floppies , bluetooth, CD/DVD recorders, 3G modem, finally, the list of available equipment in the market is huge, and its use due to the easy portability of information only grows. Proportionally, increasing the risk of leakage information.

Therefore, this article seeks to bring the attention of the reader a solution developed by the company Makrosystems - Information Technology, based in Canoinhas, Santa Catarina, with a new model of software that aims to protect the leakage of corporate information, occurring through these removable devices.
Key-words: Security Information – Removable devices – Leakage of information

INTRODUÇÃO

Os dados da sua empresa estão seguros? Dados, informações, conhecimento, representam hoje os principais ativos de qualquer organização, e administrar bem os riscos associados a esses ativos corporativos transformou-se num requisito indispensável, tanto pelo alto valor associado a esses ativos quanto pelos impactos negativos que a destruição, alteração ou divulgação indevida de informações podem trazer para as finanças e para a imagem da organização, tais como penalização por não-conformidade com a lei, perda de credibilidade no mercado, prejuízos decorrentes de fraudes,venda de segredos de negócio para concorrentes etc.

Garantir a segurança da informação exige avaliar cuidadosamente os riscos no contexto mais amplo possível, procurando entender questões como "o que proteger", "de que ameaças", "por que razão". Na Era do Conhecimento, a proteção da informação é prioridade fundamental para a continuidade dos negócios num mundo altamente competitivo.

1. Conceitos e definições sobre segurança da informação

Algumas das definições do dicionário Magno (p. 800) para a palavra segurança é "proteção", "garantia", "estabilidade em determinada condição ou situação", ou seja, pode-se dizer que segurança é a condição de estar protegido de perigo ou perda.

O conceito de informação de acordo com Sêmola (2003, p. 45), pode ser definido como:

> Conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos (isto é, baseados em troca de mensagens) ou transacionais (isto é, processos em que sejam realizadas as operações que envolvam, por exemplo, a transferência de valores monetários).

Em outras palavras informação é o resultado do processamento, manipulação e organização de dados numa forma que se some ao conhecimento da pessoa que o recebe.

Atualmente o conceito de Segurança da Informação está padronizado pela norma ABNT NBR ISO/IEC 17799:2005 (2005, p. ix), " a segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio." Esta norma rege também que a segurança da informação é caracterizada pela garantia de três fundamentos essenciais: confidencialidade, integridade e disponibilidade.

a) Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas.
b) Integridade: propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).
c) Disponibilidade: garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna.

2. Gestão de Risco

> Gestão de risco é o conjunto de processos que permite às organizações a identificar e implementar as medidas de proteção necessárias para diminuir os riscos a que estão sujeitos os seus ativos de informação, equilibrá-los com os custos operacionais e financeiros envolvidos (BEAL, 2008, p. 11).

Informações básicas de segurança já são difundidas por muitas empresas, e acreditando que os problemas com segurança só tendem a aumentar, os profissionais devem se preparar para manter os ativos de informação a salvo de ameaças à sua confidencialidade, integridade e disponibilidade. Dentro da gestão de risco, conhecendo as ameaças e vulnerabilidades a que estão sujeitas as informações, bem como os impactos que podem advir do comprometimento de sua segurança, torna-se mais bem fundamentada e confiável a tomada de decisão sobre como agir com a proteção dos dados. Assim sendo, dentro do contexto da segurança da informação, as definições e terminologias que facilitam a análise do risco são:

2.1 Ativo: Tudo o que representa valor para o negócio da instituição, como pessoas, aplicações, tecnologia e informações (ALVES, 2006).

Para maior entendimento desta definição, podemos observar na pesquisa realizada em 2008 pela *Sandisk Corporation* (líder global em fornecimento de memória flash), o resultado de um novo estudo demonstrando os riscos de uso de drives flash USB, inseguros em organizações empresarias. Nesta pesquisa usuários revelaram que os arquivos de dados mais provavelmente copiados em drives flash pessoais são:
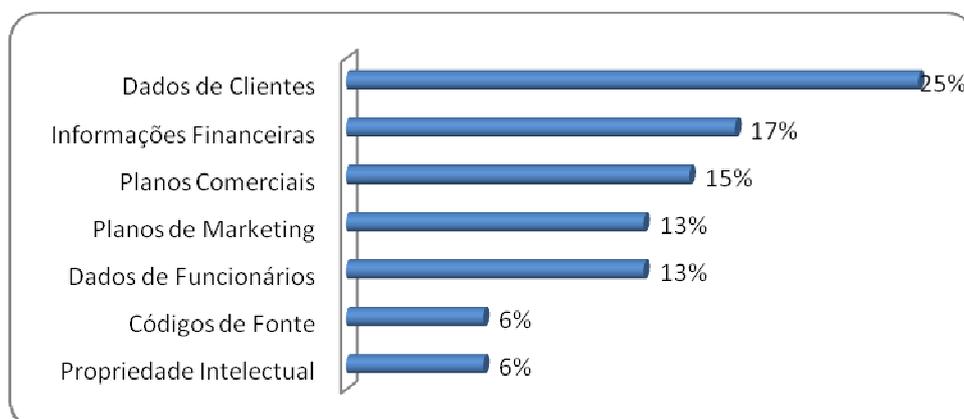
Gráfico 1 – Dados mais copiados em drives flash pessoais.
Fonte: *Sandisk Corporation* (2008)

Analisando o gráfico, a proteção dos ativos da informação, contra o acesso indevido causado pelos dispositivos amovíveis é importante, pois representam um risco significativo. Para reduzir esses riscos à monitoração de dados e o cumprimento de normas e políticas formalmente definidas, permitiriam que as organizações aproveitassem os benefícios de produtividade da maior portabilidade das informações.

2.2 Ameaças: Expectativa de acontecimento acidental ou proposital, causado por um agente, que pode afetar um ambiente, sistema ou ativo de informação (BEAL, 2008, p. 14). Ex: Hackers, concorrentes, etc.

> A todo instante os negócios, seus processos e ativos físicos, tecnológicos e humanos são alvo de investidas de ameaças de toda ordem, que buscam identificar um ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada. (SÊMOLA, 2001, p. 18).

A 9ª edição da Pesquisa Nacional de Segurança da Informação realizado pela empresa Módulo *Security* em 2003, apresentou as principais ameaças de segurança da informação no Brasil. A metodologia usada contou com a coleta de dados de respostas presenciais e via on-line. No total, a pesquisa quantitativa teve uma amostra de 682 questionários, coletados entre março e agosto de 2003, junto a profissionais ligados às áreas de Tecnologia e Segurança da Informação.
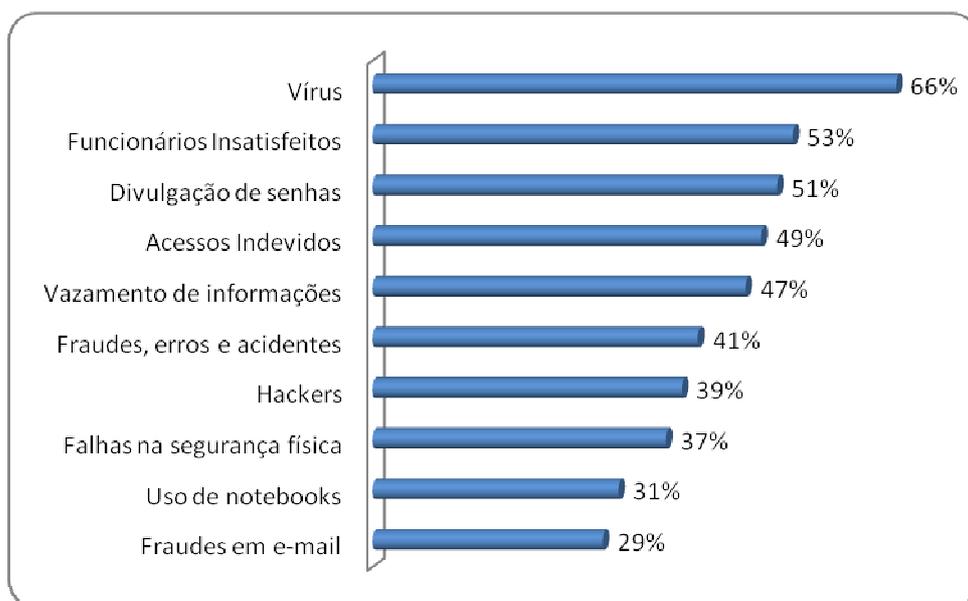
Gráfico 2 – Principais ameaças a Segurança da Informação.
Fonte: Módulo *Security* (2003)

Nota-se que grande parte das invasões realizadas nas empresas tem participação de funcionários ou ex-funcionários. A tecnologia dos dispositivos amovíveis facilita muito essas atividades, ou seja, um funcionário pode abrigar mais de 30 milhões de registro de clientes de uma empresa em um pen drive, e ninguém precisa entender de conexão em rede, basta espetar um chaveirinho e fazer o transporte físico das informações para qualquer lugar, inclusive para fora da empresa, ou até mesmo para o seu concorrente. E igualmente, um funcionário descontente pode acessar uma informação estratégica da empresa, ou uma fórmula de um produto, ou cadastro de clientes, enfim, e apagá-las, ou divulgar as informações, prejudicando a mesma no mercado.

A 9ª edição da Pesquisa Nacional de Segurança da Informação, apresentou também os principais responsáveis por ataques e invasões, como mostra gráfico 3.
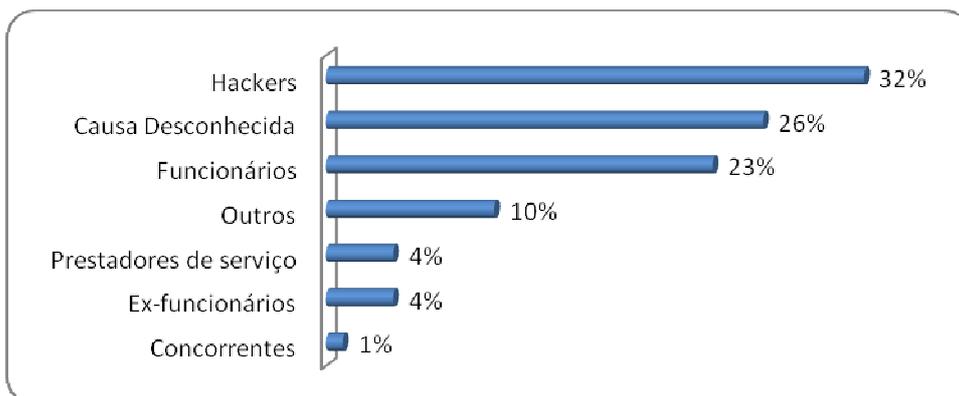
Gráfico 3 – Principais responsáveis por ataques e invasões.
Fonte: Módulo *Security* (2003)

O fator negativo que podemos observar neste gráfico é que 26% das empresas não conseguem sequer identificar a origem dos ataques e invasões. Dado este que revela a falta de controle da perda, fuga ou roubo das informações.

1.1 **Vulnerabilidade:** Fragilidade ou conjunto de falhas que poderiam ser exploradas por uma ameaça para concretizar um ataque (ALVES, 2006; BEAL, 2008).

A análise de riscos é uma importante ferramenta para diagnosticar a situação da segurança na empresa e recomendar ações para cada vulnerabilidade mapeada. O ideal seria fazer uma avaliação para classificar os riscos, monitorando onde residem as informações confidenciais da empresa, e revisar o perfil do usuário que pode acessá-las. Outro item importante é o treinamento dos funcionários para que eles entendam quais são os reais riscos de um roubo de informações.

Segundo pesquisa realizada, conforme mostra gráfico 4, 51% das pessoas utilizam dispositivos amovíveis para copiar informações confidencias da empresa, e 39% já perderam dispositivos amovíveis. Ou seja, além dos dispositivos amovíveis representarem uma fragilidade ao acesso às informações, perde-los só pioram a situação, pois deixam a empresa ainda mais vulnerável, sabendo-se que seus dados podem cair nas mãos de qualquer pessoa.
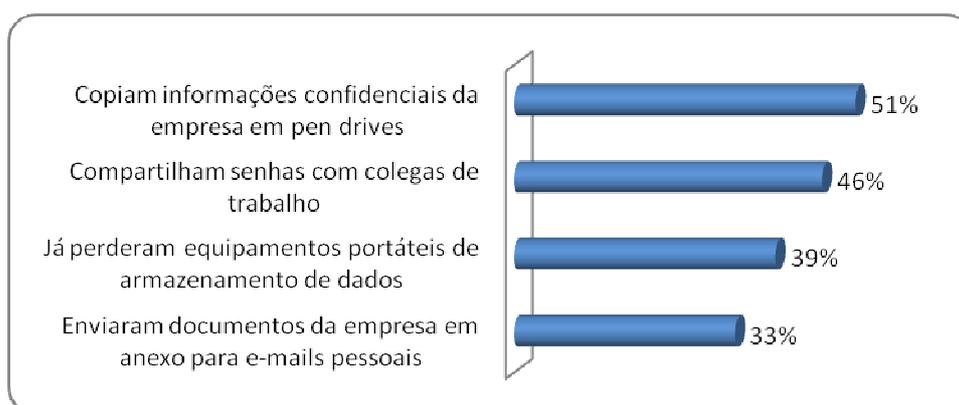
Gráfico 4 – Práticas indevidas dos funcionários colocam em risco muitos dados corporativos.
Fontes: *McAfee,Ovum e Ponemon Institute* (2008) - Base: 893 respostas (mundo)

Segundo uma pesquisa da empresa de segurança digital *McAfee*, os pen drives já são o segundo meio mais utilizado para transportar documentos e dados corporativos para fora da companhia, só perdem para os laptops. Mas, ao contrário dos PCs portáteis, os chaveiros de memória são difíceis de controlar e são encarados de forma casual. São raras as empresas que exigem que os dados por eles transportados sejam protegidos.
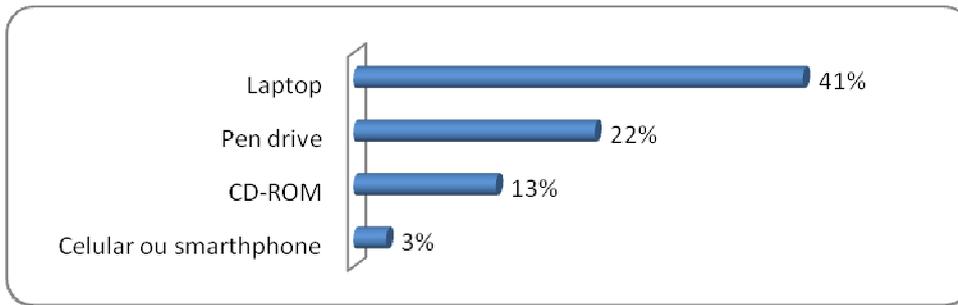
Gráfico 5 – Aparelhos portáteis mais utilizados para transportar dados corporativos.
Fontes: *McAfee, Ovum e Ponemon Institute* (2008) - Base: 893 respostas (mundo)

2.3 Impacto: Resultado de um incidente de segurança, que poderá acarretar perdas ou danos pequenos, médios ou grandes (ALVES, 2006, p. 4).

Tendo identificado as ameaças e as vulnerabilidades dos ativos da empresa, podem-se identificar os impactos que estes podem causar na mesma.

A 9ª Pesquisa Nacional de Segurança da Informação apresentou o impacto causado por ataques ou invasões, conforme mostra gráfico abaixo.
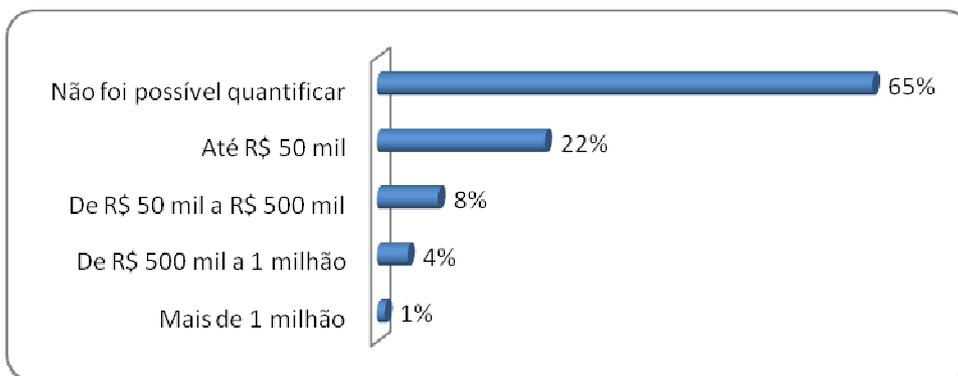
Gráfico 6 – Impacto: Perdas financeiras
Fonte: Módulo *Security* (2003)

As maiorias das empresas estão cientes de que, o vazamento de dados pode resultar em furto de identidade, prejuízo a propriedade intelectual, perda de segredos comerciais, danos financeiros e de relações públicas, informações estas, importantes para as organizações. Embora haja consciência dos riscos potencias com dispositivos amovíveis, as organizações precisam de políticas, instruções e soluções tecnológicas mais eficazes, a fim de reduzir os riscos de modo suficiente, permitindo, ao mesmo tempo, que as empresas aproveitem os benefícios de produtividade da maior facilidade do transporte da informação.

A 9ª Pesquisa Nacional de Segurança da Informação, apresentou os principais obstáculos para implementação da segurança, conforme ilustra gráfico a seguir.
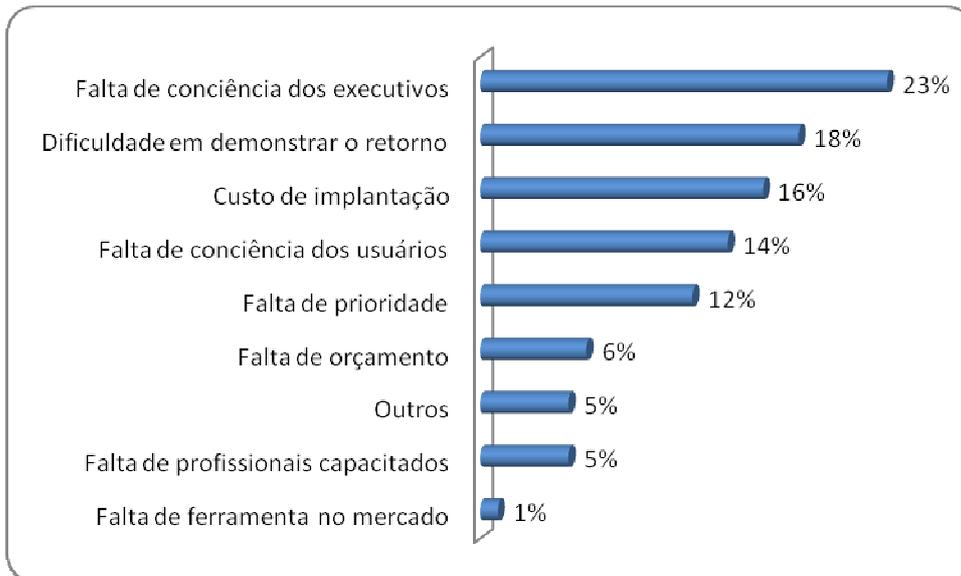
Gráfico 7 – Principais obstáculos para implementação da segurança.
Fonte: Módulo *Security* (2003)

Podemos constatar que a falta de consciência dos executivos representados por 23%, ainda é o maior obstáculo para a implementação da segurança, dado este que revela o grau de descuido com relação ao tratamento dos riscos para a segurança da informação.

A dificuldade em demonstrar o retorno representado por 18% é conseqüência do primeiro, pois com a falta de consciência dos executivos, muitas empresas acabam sofrendo os impactos causados pela perda, fuga ou roubo dos dados, e sem um gerenciamento das informações não tem como verificar, provar, ou mesmo descobrir, quem, quando, ou como houve o vazamento da mesma. Assim, somente depois disso, as empresas conseguem visualizar tamanha importância da segurança da informação.

2. Dispositivos amovíveis

Amovível é todo objeto que não sendo fixo pode ser retirado do local onde se encontre. Assim, dispositivo amovível é um dispositivo de armazenamento de informação (dados), que não está diretamente ligado ao computador, por isso pode ser transportado facilmente.

A seguir, uma série de dispositivos amovíveis que podem facilmente abrir as portas à fuga das informações para as mãos erradas:

2.1 Pen drive - dispositivo de armazenamento constituído por uma memória flash tendo aparência semelhante à de um isqueiro ou chaveiro. Tem capacidade atual de armazenamento que variam de 64 Mb à 1 Tb. Conexão pela porta USB.

2.2 Celulares e Smartphones – telefone celular com funcionalidades avançadas que podem ser estendidas por meio de programas executados no Sistema Operacional. Em sua maioria possuem cartões de memória embutidos. Conexão através da porta USB ou Bluetooth.

Os celulares guardam tantos dados confidenciais e importantes para o negócio da empresa quanto a rede de computadores das mesmas e esses aparelhos também se conectam à internet, enviam e recebem e-mails, permitem a leitura de arquivos de PDF, Power Point, entre outros.

Dos modelos mais simples aos mais sofisticados, os celulares adquiriram uma capacidade de processamento comparada a de um computador. Para muitos executivos, o celular é a forma mais simples e discreta de levar trabalho para todos os lados. Alguns até preferem carregar seus smartphones, aparelhos que são um misto de celular e computador de mão, a notebooks.

O risco aumenta à medida que o celular tem mais recursos. Normalmente, modelos com a tecnologia bluetooth, que permite a transmissão de dados entre aparelhos por radiofrequência em curtas distâncias, são alguns dos mais sensíveis a incidentes de segurança.

2.3 **Personal digital assistants (PDAs ou *Handhelds*), palmtops** - é um computador de dimensões reduzidas dotado de grande capacidade computacional, cumprindo as funções de agenda e sistema informático de escritório elementar, com possibilidade de interconexão com um computador pessoal e uma rede informática sem fios para acesso a correio eletrônico e internet. Os PDAs de hoje possuem grande quantidade de memória e diversos softwares para várias áreas de interesse. Os modelos mais sofisticados possuem modem (para acesso à internet), câmera digital acoplada (para fotos e filmagens), tela colorida, rede sem fio embutida. Conexão através da porta USB ou Bluetooth.

2.4 **Bluetooth -** é uma especificação industrial para áreas de redes pessoais sem fio (*Wireless personal area networks* - PANs). O Bluetooth provê uma maneira de conectar e trocar informações entre dispositivos como telefones celulares, notebooks, computadores, impressoras, câmeras digitais e consoles de videogames digitais através de uma freqüência de rádio de curto alcance globalmente não licenciada e segura.

Desavisados usuários da tecnologia Bluetooth, que permite a troca de informações sem fio, podem capturar o sinal de um aparelho estranho indevidamente. Ou, pior, deixarem abertas portas para que outros captem o sinal de seu aparelho e acessem suas informações. O usuário deve ter cuidado de só habilitar o Bluetooth na hora de fazer a transferência de dados. O problema é que muitos aparelhos já saem de fábrica habilitados, e se tornam presas fáceis quando nas mãos de usuários menos preocupados com questões de segurança.

2.5 **Gravadores de CD e DVD -** equipamento utilizado para gravar mídias de CD e DVD onde a capacidade de armazenamento variam de 700 Mb à 10 Gb. O gravador de CD ou DVD segundo Filho (2004, p.34):

> "[...] é perigoso, pois pode levar de uma vez uma grande quantidade de dados em um volume físico muito pequeno, que só uma revista minuciosa poderia descobrir. Para piorar, existem os CD-Card, que cabem em uma carteira, e podem levar uma dezena de Mega Bytes. Com a ajuda de compactadores, a massa de dados pode ser maior ainda.

2.6 **Modem 3G -** as tecnologias 3G permitem às operadoras da rede oferecer a seus usuários uma ampla gama dos mais avançados serviços, já que possuem uma capacidade de rede maior por causa de uma melhora das mesmas. Entre os serviços, há a telefonia por voz e a transmissão de dados a longas distâncias, tudo em um ambiente móvel. Normalmente, são fornecidos serviços com taxas de 5 a 10 Megabits por segundo. As redes 3G permitem telefonia móvel de longo alcance e evoluíram para incorporar redes de acesso à Internet em alta velocidade e Vídeo-telefonia. Conexão através da porta USB.

2.7 **HD Externo:** mesma capacidade dos HDs internos, só que com tamanho reduzido. Conexão pela porta USB.

2.8 **Cartão de memória** ou **cartão de memória flash:** é um dispositivo de armazenamento de dados com memória flash utilizado em videogames, câmeras digitais, telefones celulares, palms/PDAs, MP3 players, computadores e outros aparelhos eletrônicos. Podem ser regravados várias vezes, não necessitam de eletricidade para manter os dados armazenados, são portáteis e suportam condições de uso e armazenamento mais rigorosos que outros dispositivos baseados em peças móveis.

MATERIAIS E MÉTODOS

A metodologia empregada para o desenvolvimento deste artigo foi baseado na pesquisa bibliográfica, compreendendo um estudo exploratório e coleta de dados empíricos, retirados de pesquisas quantitativas, realizadas por empresas especializadas e certificadas em tecnologia para Gestão de Riscos e Segurança da Informação.

O trabalho comparou a teoria com fatos reais vivenciados pelas corporações visando contribuir com as empresas, e apresentou uma nova proposta de software desenvolvida pela empresa Makrosystems – Tecnologia de Informação, com sede em Canoinhas, Santa Catarina, verificando que a proposta feita fornece uma solução favorável aos problemas apresentados.

RESULTADOS E DISCUSSÃO

A velocidade da informação que é necessária nos dias de hoje fizeram com que dispositivos de diferentes redes e diferentes tecnologias se comunicassem entre si, celulares se conectam com computadores, aparelhos de som tocam músicas direto de pen drives, TV's exibem vídeos e fotos direto da câmera digital, e muitos outros exemplos mostram a diversidade e a facilidade no transporte da informação. Mas junto com esses benefícios, vieram também às preocupações. Como garantir que os dados confidenciais das empresas não sejam acessados e copiados? Como garantir que uma pessoa não coloque propositadamente um vírus na rede? Como garantir que o funcionário não esteja trazendo tarefas particulares para dentro da empresa?

O desenvolvimento do software Makrolock partiu deste principio, pois essas tecnologias em sua maioria são novas, conseqüentemente seus problemas também, e as soluções para isso ainda são muito poucas.

O software gerencia o uso de dispositivos que se utilizam da porta USB, como pen drive, celulares, gravadores CD/DVD, conforme mostra figura abaixo, evitando assim o roubo de informações.

Figura 1 – Bloqueia ou desabilita o uso de dispositivos amovíveis

O gerenciamento é feito através do controle de entrada e saída de dados que for conectado pela porta USB, através de três funções: liberado, somente leitura e bloqueado.

A opção, “liberado” deixa a USB em seu estado normal, mas faz a geração do LOG, ou seja, disponibiliza um registro de verificação detalhado de tudo o que entra e tudo o que sai como, nome do arquivo, data e hora da cópia, qual o seu destino, qual sua origem, em que computador foi feito. Assim, mesmo a porta USB estando liberado, a empresa terá como saber, o que saiu por aquele computador, ou por onde o vírus entrou, que material o funcionário trouxe para dentro da empresa, se é profissional ou particular. A opção “somente leitura” faz com que o usuário possa trazer informações para dentro do computador, mas não pode retirá-las. O log também esta disponível nesta opção. A opção, “bloqueado” deixa a USB inoperante para esses dispositivos.

Mas nem só de USB vive a conexão. Muitos dispositivos têm a tecnologia Bluetooth, que nada mais é que uma rede pessoal onde dois dispositivos ou mais podem se comunicar sem precisar qualquer fio ou porta para isso. O sistema também bloqueia esse serviço, bloqueando esse tipo de conexão, deixando o serviço inoperante.

Gravadores de CD e DVD também é uma dor de cabeça com relação ao transporte de informação. A maioria dos notebooks já vem de fábrica com esse dispositivo e os leitores de CD estão praticamente fora de mercado. Com relação a isso o software bloqueia todo programa de gravação de CD/DVD, deixando à gravadora funcionando apenas como um leitor.

Palmtops, smartphones, enfim, uma série de dispositivos com cada vez mais recursos e com mais capacidade de armazenamento está aparecendo e o Makrolock também gerencia a conexão com esses dispositivos de uma maneira parecida com a porta USB.

Apesar de o disquete ter caído em desuso, muitas empresas ainda o utilizam, e a forma de gerenciamento é igual da porta USB.

Os cartões de memória muito difundidos principalmente através das maquinas fotográficas digitais também fazem parte desse gerenciamento, pois esses cartões estão cada vez mais sendo utilizados para o transporte de dados.

Outra vantagem, é que o sistema funciona através de um servidor e múltiplos clientes, centralizando o gerenciamento, assim todas as portas dos dispositivos amovíveis da rede ficam centralizadas em um único computador.

Com esse gerenciamento, é possível ter o controle das informações ou dados que entram ou saem da empresa.

CONSIDERAÇÕES FINAIS

Este artigo procurou oferecer uma visão abrangente do problema da segurança da informação, inserindo-o no contexto da gestão de risco, visando entender as ameaças, vulnerabilidades e impactos que rondam as informações corporativas, causados pelos dispositivos amovíveis.

O artigo relatou a importância das informações corporativas, evidenciando os principais responsáveis pela perda, fuga ou roubo de informações, dado alarmante este, pois funcionários e ex-funcionários representam 37% dos principais responsáveis por ataques e invasões, conforme mostra gráfico 7.

O artigo mostrou os principais dispositivos amovíveis usados para transportar as informações, deixando as empresas vulneráveis, pois estes equipamentos são difíceis de ser controlados. Apresentou

também, as principais informações copiadas das empresas, e finalmente as conseqüências ocorridas com o vazamento das mesmas.

O vazamento das informações nunca foi tão fácil, e o despreparo das corporações é algo claro e evidente, pois pesquisa apresentada pelo gráfico 7, mostra que um dos principais obstáculos para a implementação da segurança é a falta de conscientização dos executivos.

O pequeno número de soluções que existem até o momento é algo que assusta também, mas é algo compreensivo, pois só agora essa tecnologia acabou se difundindo no mundo corporativo, devido à necessidade cada vez maior, da mobilidade e praticidade no transporte das informações.

Temos que ter a consciência que nos dias de hoje, a velocidade da informação é importantíssima, mas o controle da informação é muito mais. Alguns anos atrás as empresas só se preocupavam com servidores de internet, firewall, sistemas de backups, mas hoje, além dessas preocupações que já são conhecidas, as empresas têm que se preocupar também, com os dispositivos amovíveis, que crescem a cada dia numa velocidade avassaladora, com mais e mais facilidades para conexão, e um controle disso se torna tão ou mais importante dos que os citados anteriormente.

O artigo procurou também contribuir com o leitor apresentando uma solução de Software de segurança de dispositivos amovíveis, desenvolvido pela empresa Makrosystems, para solucionar o problema contra estes riscos em potencial.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISSO/IEC 17799:2005 – Tecnologia da Informação - Técnicas de Segurança - Código de Prática para a gestão da segurança da informação.** Rio de Janeiro: ABNT, 2005.

ALVES, Gustavo Alberto. **Segurança da Informação -** Uma visão inovadora da gestão**.** Rio de Janeiro: Editora Ciência Moderna Ltda, 2006.

BEAL, Adriana. **Segurança da Informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. 1. ed. 2005; 2.reimpressão 2008. São Paulo: Atlas, 2008.

CASTRO, Cláudio de Moura. **A prática da pesquisa**. São Paulo: McGraw-Hill, 1977.

FILHO, João Rocha Braga. **Os dados da sua empresa estão seguros? Duvido!** Rio de Janeiro: Brasport Livros e Multimídia Ltda, 2004.

MAIA, Raul. **Magno – Dicionário Brasileiro da Língua Portuguesa.** São Paulo: ed. Edipar Edições e Participações Ltda. [1995].

SÊMOLA, Marcos. **Gestão da Segurança da Informação**: uma visão executiva. Rio de Janeiro: Campus, 2003.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**. 2. ed. Rio de Janeiro: Campus, 2003.

FUSCO, Camila. **Plantão Info:** Tão pequeno e tão perigoso. Disponível em: <http://info.abril.com.br/aberto/infonews/072008/07072008-13.shl>. Acesso em 10 jan. 2008.

MAKROSYSTEMS – Tecnologia de Informação. **Software Makrolock.** Disponível em: <http://www.makrosys.com.br/?pg=produto&id=11>. Acesso em 12 jan. 2008.

MÓDULO TECHNOLOGY FOR RISK MANAGEMENT. **9ª Pesquisa Nacional.** Disponível em: <http://www.modulo.com.br/site?sid=22&lng=br>. Acesso em: 12 jan. 2008.

SANDISK STORE YOUR WORLD IN OURS. **Pesquisa Realizada Pela SanDisk Revela Organizações em Risco por uso de Drives Flash USB Inseguros. O Uso é Maior Que o Dobro Esperado Pela Área de TI Empresarial.** Disponível em: <http://br.sandisk.com/Corporate/PressRoom/PressReleases/PressRelease.aspx?ID=4094>. Acesso em: 10 jan. 2008.

WIKIPÉDIA, a enciclopédia livre. **Segurança da Informação.** Disponível em: <http://pt.wikipedia.org/wiki/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o>. Acesso em: 12 jan. 2008.

NOTAS

[1] Artigo de conclusão do Curso de Pós Graduação em MBA em Gestão de Excelência nas Organizações, ministrado pela Universidade do Contestado – UnC Canoinhas. Sob orientação do professor Reinhardt Sievers.

[2] Peruci – Formada em Administração de Empresas com Habilitação em Comércio Exterior. E-mail: mperuci@yahoo.com.br

[3] Montagnana – Formado em Tecnologia em Celulose e Papel – E-mail: paulosergio@canoinhas.com.br

[4] Silveira – Formada em Administração de Empresas e Pós Graduada em GBA Global Business Administration. E-mail: simone@fvital.com.br